2018 Statewide Glossary Update Summary

Added the following terms:

- **Advanced Persistent Threat (APT)** – A network attack in which an unauthorized person gains access to a network and remains undetected for a long period of time in order to steal data, rather than cause damage to the organization. The characteristics of APT are as follows:
    - Purposeful with defined objectives
    - Resourceful
    - Sophisticated methods and technology
    - Substantially funded for ongoing efforts
- **Breach** – An incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner. A data breach can occur with a small company or a large organization, and it may involve sensitive, proprietary, or confidential information, such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. Also called Cyber Breach or Data Breach.
- **Cloud Access Security Broker (CASB)** – A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to monitor all activity and enforce its own security policies. It can offer a variety of services, including but not limited to monitoring user activity, warning administrators about potentially hazardous actions, enforcing security policy compliance, and automatically preventing malware.
- **Command and Control (C2, C&C)** – Command-and-control servers issue commands and controls to compromised systems (often Internet-connected computers that then form zombie armies known as botnets). These communications can be as simple as maintaining a timed beacon or "heartbeat" so that the operators running the attack can keep an inventory of systems they have compromised within the target network, or use them for more malicious actions, such as remote control or data exfiltration. While the command-and-control server is used to control the system on the inside of the target organization, it is usually the compromised host that initiates the communication from inside the network to a command-and-control server on the public Internet.
- **Container-based encryption** provides a more fine-grained approach to the encryption of data/information on mobile devices, including for example, encrypting selected data structures such as files, records, or fields. (***Note:*** *This is added as a sub-item to the term "Encryption"*)
- **Continuous Monitoring** – Continuous monitoring of information systems is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. This involves collecting and analyzing information regularly from multiple sources in accordance with pre-established metrics in order to manage risk as appropriate for each organizational tier.
- **Corrective Action Plan (CAP)** – A corrective action plan (CAP) is a step by step plan of action and schedule that is developed to correct a process or area of non-compliance, that often includes the most cost-effective actions that can be implemented to correct errors.
- **Department of Homeland Security (DHS)** – A federal agency that was created through the integration of all or part of twenty-two different federal departments and agencies into a unified, integrated department whose mission is to secure the nation from the many threats we face.

2018 Statewide Glossary Update Summary

- **Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)** – The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) was established by the EIS-GCC to support the cybersecurity needs of the elections subsector. Through the EI-ISAC, election agencies will gain access to an elections-focused cyber defense suite, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products, and tools for implementing security best practices.
- **Exception Process** – An acknowledgement or request for an agency to proceed contrary to an established law, policy, or standard practice. Exceptions can be for procurement, security or standards and they require DIT or State CIO reporting and/or approval.
- **Exploit** – An attack that takes advantage of vulnerabilities in an application, operating system (OS), network, or hardware. Exploits usually take the form of software or code that aim to gain control of computers or steal data.
- **Federal Emergency Management Agency (FEMA)** – A federal agency that coordinates the federal government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. FEMA's mission is to lead America to prepare for, prevent, respond to and recover from disasters with a vision of "A Nation Prepared".
- **Homeland Security Exercise and Evaluation Program (HSEEP)** – A Department of Homeland Security (DHS) program that provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning.
- **Indicators of Attack (IOA)** – Indicators of attack (IOA) are similar to indicators of compromise (IOCs), but rather than focusing on forensic analysis of a compromise that has already taken place, indicators of attack focus on identifying attacker activity *while* an attack is in process.
- **Indicators of Compromise (IOC)** – Indicators of compromise (IOCs) are pieces of digital data, such as that found in system log entries or files, that identify potentially malicious activity on a system or network.
- **Kill Chain** – The Cyber Kill Chain is a model for identification and prevention of cyber intrusion activity. The model identifies what cyber adversaries must complete to achieve their objective. The kills chain involves several threat stages that are as follows:
    - Reconnaissance: Intruder selects a target, researches it, and attempts to identify vulnerabilities in the target network.
    - Weaponization: Intruder creates a remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities.
    - Delivery: Intruder transmits weapon to target (e.g., via e-mail attachments, websites or USB drives).
    - Exploitation: Malware weapon's program code triggers, which takes action on target network to exploit vulnerability.
    - Installation: Malware weapon installs access point (e.g., "backdoor") usable by intruder.
    - Command and Control: Malware enables intruder to have "hands on the keyboard" persistent access to target network.

- Actions on Objective: Intruder takes action to achieve his/her goals, such as data exfiltration, data destruction, or encryption for ransom.

The actions to take to defend against the cyber kill chain are as follows:

- Detect: determine whether an attacker is poking around
- Deny: prevent information disclosure and unauthorized access
- Disrupt: stop or change outbound traffic (to attacker)
- Degrade: counter-attack command and control
- Deceive: interfere with command and control
- Contain: network segmentation changes

- **Maximum Acceptable Outage (MAO)** – This is the timeframe during which a recovery must become effective before an outage compromises the ability of an organization to achieve its business objectives and or survival. (FEMA) *See,* MTD; MTA.
- **Maximum Tolerable Downtime (MTD)** – The maximum number of hours for which it is acceptable that a function can be interrupted following a continuity event. (FEMA) *See*, Recovery Time Objective; Maximum Acceptable Outage.
- **Maximum Time in Alternative Operations (MTA)** – *See*, Maximum Acceptable Outage (MAO)
- **Multi-State Information Sharing & Analysis Center (MS-ISAC)** – The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for U.S. State, Local, Territorial, and Tribal (SLTT) governments. It collects, analyzes and disseminates actionable threat information to its members and provides members with tools to mitigate risks and enhance resiliency.
- **Nation State** – A nation state threat actor is a type of Advanced Persistent Threat (APT). The nation state threat actor receives direction and support from an established nation state (government). The line between nation-state cyber activity and cybercrime is often blurred as organized crime groups are afforded a degree of support.
- **Nationwide Cybersecurity Review (NCSR)** – A free, anonymous, annual self-assessment survey that is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and is sponsored by the Department of Homeland Security (DHS) and the MS-ISAC.
- **Ransomware** – A type of malicious software (malware) that threatens to publish the victim's data or prevents users from accessing their system or personal files unless a ransom is paid. Ransomware typically encrypts the victim's data and withholds the decryption key until the ransom is paid. Sometimes, the criminal does not provide the decryption key even if the ransom is paid; therefore, law enforcement agencies state that it is best practice to *not* pay the ransom.
- **Reconnaissance** – Gathering information on a target before the actual attack starts. Active reconnaissance is an attack in which an adversary engages a targeted network or system to gain information about vulnerabilities. Passive reconnaissance is an attempt to gain information about targeted computer systems and networks without actively engaging with those systems.
- **Resilience** – The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (DHS/FEMA)

Examples of resilience measures include the following:

- Developing a business continuity plan
- Having a generator for back-up power
- Using building materials that are more durable.

- **Security Information and Event Management (SIEM)** – Technology that supports threat detection and security incident response through the real-time collection and historical analysis of security events from a variety of data sources. A SIEM also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources.
- **Threat and Hazard Identification and Risk Assessment (THIRA)** – A three-step risk assessment process of the Department of Homeland Security (DHS) that helps communities answer the following questions:

  - What threats and hazards can affect our community?
  - If they occurred, what impacts would those threats and hazards have on our community?
  - Based on those impacts, what capabilities should our community have?

  The THIRA helps communities understand their risks and determine the level of capability they need to address those risks. The outputs form this process lay the foundation for determining a community's capability gaps as part of the Stakeholder Preparedness Review.

Updated the following terms (*new definition provided below*):

- **Agency –** Any department, institution, commission, committee, board, division, bureau, office, officer, or official of the State of North Carolina that is subject to the State CIO's policies and standards. The term does not include a State entity excluded from coverage under G.S. § 143B 1300, unless that State entity elects to be covered.
- **Authentication –** The process of determining whether someone or something is, in fact, who or what it is declared to be (verifying the identity of the user) based upon credentials provided such as a user ID and password combination. It is the act of identifying or verifying the eligibility of a workstation, originator, or individual to access specific categories of information.
- **Authorization –** The process of granting a user access to information, a system or an application. Often access privileges are granted based on the role the user has in relation to the organization and/or the system to be accessed.
- **Authorized User** – A person, system, application or defined group that has been authenticated to an information technology (IT) system and granted access only to those resources which he or she has been permitted to use.
- **Delegation of Authority** – Delegations of Authority are formal documents that specify the activities that those who are authorized to act on behalf of the agency head or other key officials may perform. Delegations of authority document the legal authority for officials—including those below the agency head—to make key policy decisions during a COOP situation. (FEMA)

2018 Statewide Glossary Update Summary

- **File Transfer Protocol (FTP)** – A TCP/IP protocol specifying the transfer of text or binary files across the network. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS) or replaced with SSH File Transfer Protocol (SFTP).
- **Information Assets** – Information relevant to an enterprise's business function, including captured and tacit knowledge of employees, customers or business partners; data and information stored in highly-structured databases, or in textual form and in less-structured databases such as messages, e-mail, workflow content and spreadsheets; information stored in digital and paper documents; purchased content; and public content from the Internet or other sources. (GARTNER)
- **(RENAME) Information Technology Incident** to **Cybersecurity Incident**
- **(RENAME/UPDATE) Mean Time Between Failure (MTBF)** to **Mean Time To Failure (MTTF)** with the following definition – "The length of time a device or other product is expected to last in operation. MTTF is one of many ways to evaluate the reliability of pieces of hardware or other technology."
- **Mobile Code** – Software that is transferred between systems and executed on a local system without explicit installation or execution by the recipient. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript, which are common installations on most end user workstations. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations and devices (e.g., tablet computers and smartphones). Active X and Java are examples of mobile code that can inadvertently breach agency network defenses.
- **Orders of Succession** – Orders of succession provide for the orderly and predefined assumption of senior agency offices during an emergency in the event that any officials are unavailable to execute their legal duties. (FEMA)
- **Phishing** – A form of fraud in which an attacker masquerades as a reputable entity or individual in an electronic communication, such as email. The attacker may use "phishing emails" to distribute malicious links or attachments to their victims that can perform a variety of functions, including the extraction of login credentials or account information, or other sensitive information
- **Redundant Array of Independent Disks (RAID)** – A data storage technology that combines multiple physical disk drive components into one or more logical units for the purposes of fault tolerance, data redundancy, and/or performance improvement.
- **(RENAME/UPDATE) Security Administrator** to **Security Liaison** with the following description: "The individual at a State agency who is assigned information technology security duties by the agency head. The liaison is appointed pursuant to G.S. § 143B-1379 and coordinates with the State CIO on information security matters."
- **(RENAME/UPDATE) Security Standard** to **Statewide Information Security Manual** with the following description: "An enterprise wide set of security standards for state information technology, adopted pursuant to G.S. § 143B-1376, to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. The security standards must be established by the State CIO."

2018 Statewide Glossary Update Summary

Removed the following terms:

- Advertise
- Assumption
- Budget
- Correctness
- Cracker
- Cracking
- Dependence
- Deviation
- Document
- Duration
- Effort
- GNU Project
- ITS
- Identification and Authentication
- Issue
- Lead
- Leadership
- Method
- Methodology
- Mistake
- North Carolina Integrated Information Network (NCIIN)
- North Carolina Department of Justice
- North Carolina Department of Public Safety
- Office of the State Auditor
- Phases
- Precedence
- Retirement
- Review
- Strong Authentication
- Stronger Authentication
- Strongest Authentication
- Team
- Vision

Miscellaneous Updates:

- **Rename** references of ***OITS*** to ***DIT***.
- **Rename** *Statewide Technical Architecture* to *Statewide Architecture Framework*.
- **Update** General Statute references.
- **Update** links as needed.